SOLUTION BRIEF

Software-Defined NIC for Remote Device Deployments

Integrating remote deployments

Versa's comprehensive network and data security capabilities allow administrators to define security functions and policies once and apply them uniformly to all Versa Secure SD-WAN nodes deployed across the network, as illustrated in Figure 1. Versa now offers the same connectivity and security functionality on a Software-Defined Network Interface Card (SD-NIC), allowing IT administrators to securely connect remote devices to the enterprise network and apply persistent zero trust network access (ZTNA), detailed cloud access control, and data leakage prevention (DLP) capabilities not found in traditional remote edge-based security solutions.

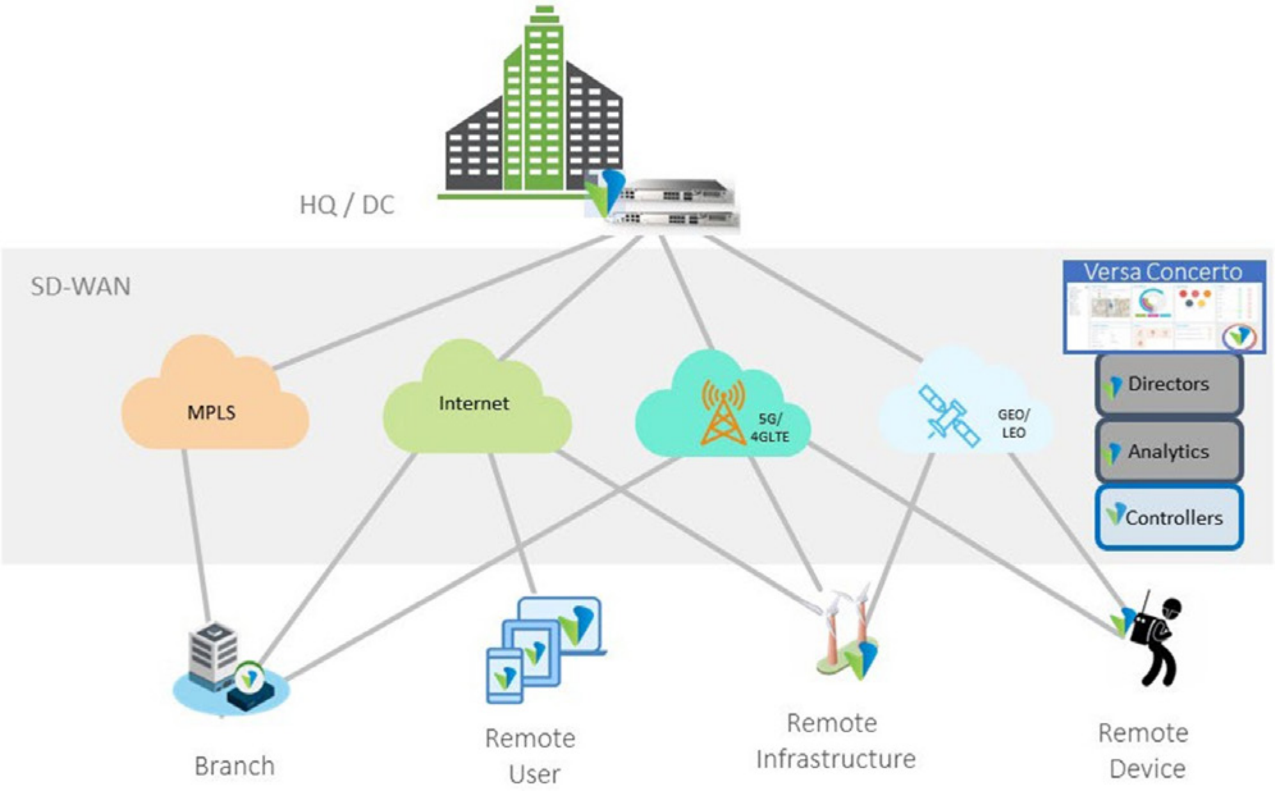


Figure 1 - Versa SD-WAN with remote device integration.

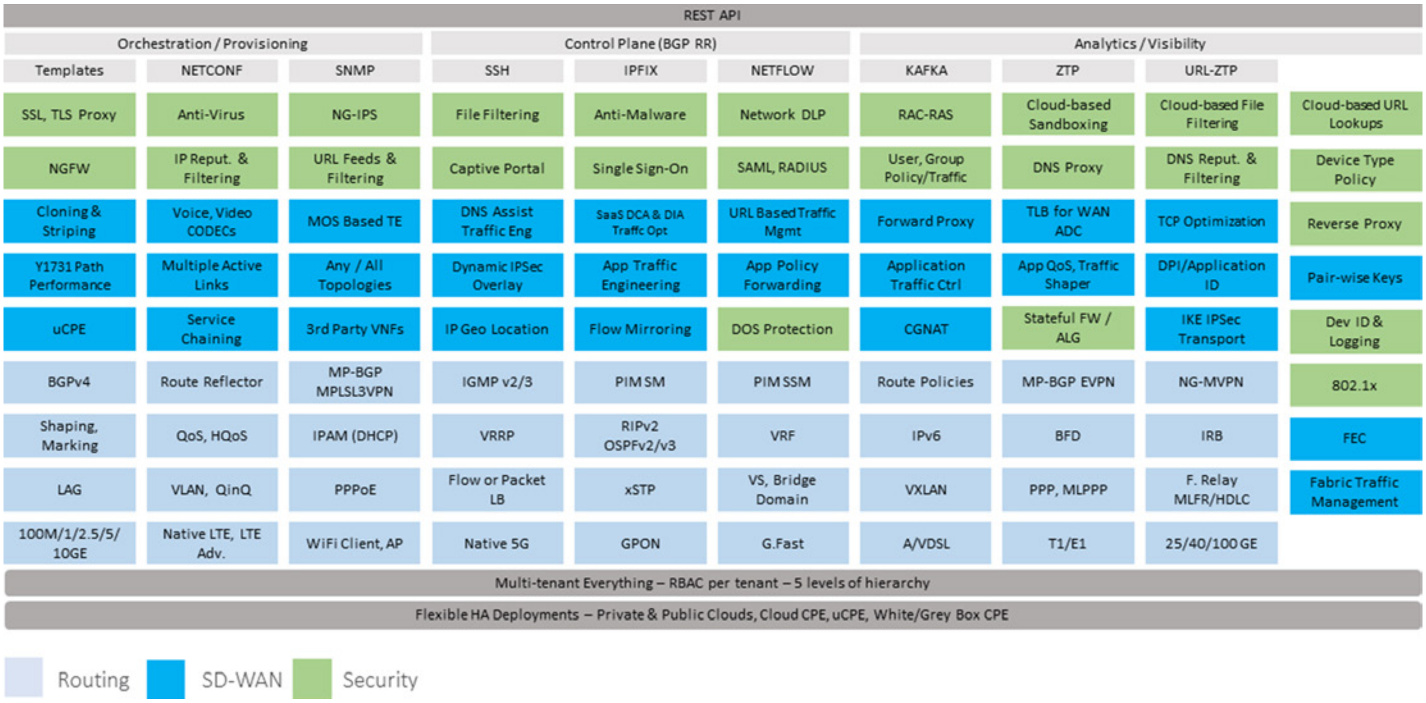
Various industries have a need to deploy servers and specialized application devices remotely with pre-installed apps that are managed centrally and enjoy robust and uniform security, often in untrusted or third-party environments, including finance, government, disaster recovery, retail, telecommunications and energy infrastructure, and defense, for use cases like:

- Trading or market news servers deployed in third-party broker environments
- ATM machines in convenience stores, gas stations or fairgrounds
- Fire, rescue and disaster response vehicles
- Pop-up retail locations
- Government field offices
- Cell towers, wind turbines, and oil rigs
- Tactical military deployments

Many of these scenarios come with tight space and limited power requirements, making a solution with multiple elements for networking and security problematic.

Security perimeter at the remote edge

Leveraging Versa's networking and security stack (see Figure 2), Versa's Software-Defined Network Interface Card (SD-NIC) effectively places the security appliance inside the remote compute device, extending the security perimeter to provide ZTNA, network security and data security to the remote network edge. Since the remote device sits in the path of the traffic, network and data security functions and status evaluations are done without the need to send the traffic out to perform them.



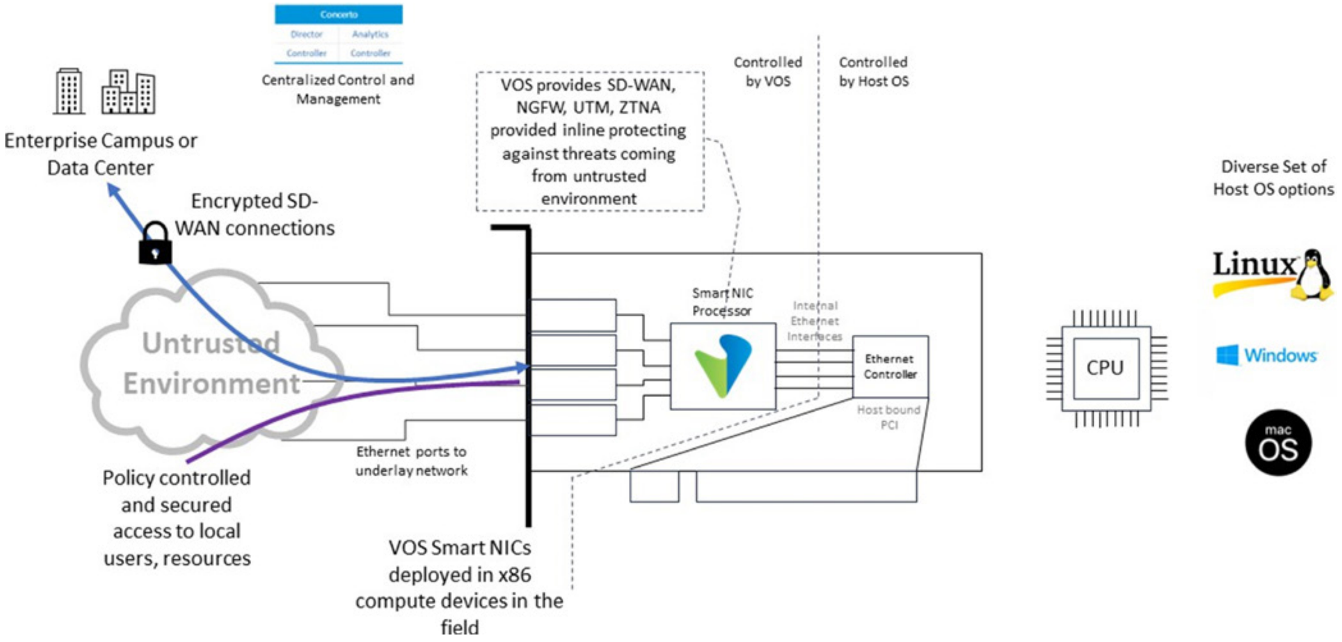
REST API									
Orchestration / Provisioning			Control Plane (BGP RR)			Analytics / Visibility			
Templates	NETCONF	SNMP	SSH	IPFIX	NETFLOW	KAFKA	ZTP	URL-ZTP	
SSL, TLS Proxy	Anti-Virus	NG-IPS	File Filtering	Anti-Malware	Network DLP	RAC-RAS	Cloud-based Sandboxing	Cloud-based File Filtering	Cloud-based URL Lookups
NGFW	IP Reput. & Filtering	URL Feeds & Filtering	Captive Portal	Single Sign-On	SAML, RADIUS	User, Group Policy/Traffic	DNS Proxy	DNS Reput. & Filtering	Device Type Policy
Cloning & Striping	Voice, Video CODECs	MOS Based TE	DNS Assist Traffic Eng	SaaS DCA & DIA Traffc Opt	URL Based Traffic Mgmt	Forward Proxy	TLB for WAN ADC	TCP Optimization	Reverse Proxy
Y1731 Path Performance	Multiple Active Links	Any / All Topologies	Dynamic IPSec Overlay	App Traffic Engineering	App Policy Forwarding	Application Traffic Ctrl	App QoS, Traffic Shaper	DPI/Application ID	Pair-wise Keys
uCPE	Service Chaining	3rd Party VNFs	IP Geo Location	Flow Mirroring	DOS Protection	CGNAT	Stateful FW / ALG	IKE IPSec Transport	Dev ID & Logging
BGPv4	Route Reflector	MP-BGP MPLSL3VPN	IGMP v2/3	PIM SM	PIM SSM	Route Policies	MP-BGP EVPN	NG-MVPN	802.1x
Shaping, Marking	QoS, HQoS	IPAM (DHCP)	VRRP	RIPv2 OSPFv2/v3	VRF	IPv6	BFD	IRB	FEC
LAG	VLAN, QinQ	PPPoE	Flow or Packet LB	xSTP	VS, Bridge Domain	VXLAN	PPP, MLPPP	F. Relay MLFR/HDLC	Fabric Traffic Management
100M/1/2.5/5/ 10GE	Native LTE, LTE Adv.	WiFi Client, AP	Native 5G	GPON	G.Fast	A/VDSL	T1/E1	25/40/100 GE	
Multi-tenant Everything – RBAC per tenant – 5 levels of hierarchy									
Flexible HA Deployments – Private & Public Clouds, Cloud CPE, uCPE, White/Grey Box CPE									

▢ Routing 🟦 SD-WAN 🟩 Security

Figure 2- Full Versa networking and security feature set

Versa SD-NIC installation and configuration options

The Versa SD-NIC, as seen in Figure 3, is based on a PCI card and is inserted into a standard PCI slot inside the remote device, just like a traditional NIC expansion card. The Versa SD-NIC card has a multicore processor on it which runs the Versa Operating System (VOS) natively, allowing Versa to instantiate a Versa SASE or SD-WAN node within the remote device.



Concerto
Director
Analytics
Controller
Controller
Centralized Control and Management
Enterprise Campus or Data Center
Encrypted SD-WAN connections
Untrusted Environment
Policy controlled and secured access to local users, resources
Ethernet ports to underlay network
VOS provides SD-WAN, NGFW, UTM, ZTNA provided inline protecting against threats coming from untrusted environment
VOS Smart NICs deployed in x86 compute devices in the field
Controlled by VOS
Controlled by Host OS
Smart NIC Processor
Internal Ethernet Interfaces
Ethernet Controller
Host bound PCI
CPU
Diverse Set of Host OS options
Linux
Windows
mac OS

Figure 3 – Versa SD-NIC runs VOS natively, placing an SD-WAN or SASE node within the remote device.

The Versa SD-NIC runs the same operating system software, VOS, found in any other Versa device. The SD-NIC therefore has the full set of Versa capabilities, including SD-WAN, SD-LAN, Next-Gen Firewall (NGFW), Unified Threat Management (UTM), Zero-trust Network Access (ZTNA), micro-segmentation, Cloud Access Security Brokerage (CASB), network-based Data Leakage Prevention (DLP) and more. The Versa operating system is application-aware, which allows for different security postures per application, segment, user, or device.

Since the Versa SD-NIC has its own CPU, memory, and storage, it can be installed into hardened devices where a traditional software agent would not be allowed. There is no dependence on the host software. Additionally, the SD-NIC includes a Trusted Platform Module (TPM 2.0). This permits the remote device to recognize the SD-NIC as valid and allows the SD-NIC to securely connect to the enterprise network.

The Versa SD-NIC is available in two different configurations today. Both configurations require no extra power and fit into a standard PCI slot. Both SD-NIC configurations have a USB 3.0 console port and a 1Gb Ethernet management interface.

The first SKU is a 2x25G/10G interface card. This SD-NIC provides for approximately 4 Gbps throughput of SD-WAN with next-gen firewall enabled and 750 Mbps throughput with UTM features enabled, and is ideal for those devices that transmit data at lower rates or utilize transport media with constrained bandwidth.

Figure 4- SD-NIC 100Gb

The second SKU is a 1x100G which is capable of a 4x25G/10G breakout configuration, as seen in Figure 4. This SD-NIC provides throughput of approximately 8 Gbps of SD-WAN with next-gen firewall enabled and approximately 1.5 Gbps throughput for SD-WAN with UTM features enabled. Given the high throughput rate with all security features enabled, this SD-NIC is capable of handling almost any remote device bandwidth needs. For higher bandwidth requirements, multiple cards can be deployed in remote devices that support multiple PCI cards.

Zero-touch provisioning and onboarding alternatives

Versa supports numerous methods to onboard a remote device, first and foremost a zero-touch provisioning capability to securely deploy and connect them to the enterprise network.. The zero-trust provisioning (ZTP) process utilizes security mechanisms to ensure that the appropriate device connects to the appropriate service before any configuration can be applied to the SD-NIC. The process utilizes factory-installed certificates with the keys from the TPM chip, connects to the Versa global provisioning system and then, based upon the serial number of the device, the Versa global provisioning system redirects to the appropriate enterprise staging environment. This can be accomplished without physical access to the device, since it automatically occurs upon boot sequence. And Versa's solution ensures that once the device does connect to the network, the user implementing the remote device is a validated and trusted entity of the enterprise.

Two alternative methods require some form of access to the device, either by ethernet cable or USB cable. URL-based provisioning requires that a URL is communicated with the field user and then the URL is activated by the field user plugging an ethernet cable into the device. The URL is an encrypted URL that has the certificate for that session encrypted in the string. This prevents the usage of this URL for any other remote device provisioning. The further option of script-based provisioning requires the USB console cable and the insertion of a script string at the command line. Note that the Versa SD-NIC has the capability to perform a secure boot. The secure boot utilizes keys stored in the SD-NIC to validate that the bootable image is a trusted image and from a trusted source.

Each one of these provisioning methods can be configured to support multi-factor authentication (MFA). With MFA a token is sent to a pre-authorized device and the field user responds to the MFA, or in the URL or script-based scenarios, enter the MFA token into the device to authenticate and authorize the provisioning.

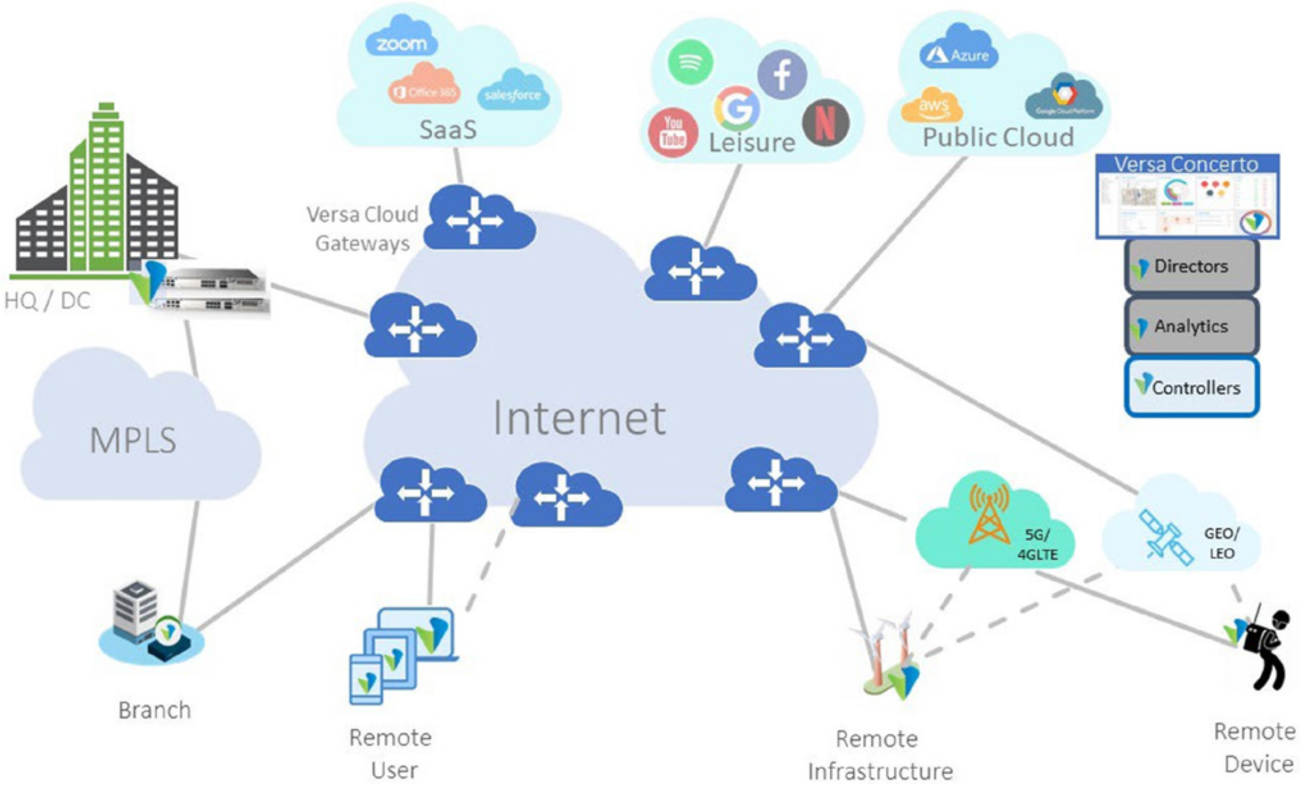


Figure 5 – Versa SASE architecture with remote device.

The remotely located compute platform can be configured to either connect to a SASE solution, as shown in Figure 5, or be part of a secure SD-WAN solution, as seen in Figure 1, over any type of transport. Versa supports connectivity over a variety of transport types. However, for most remote cases, the connectivity is either via an ethernet cable to a service provider (Internet), cellular connectivity (4GLTE or 5G), or satellite connectivity.

Zero-trust access

Versa's ZTNA provides access control to and from the remote device and the rest of the network under strict policy guidance and based on the dynamically-assessed security posture of the instance. Versa's ZTNA solution assesses the security posture of the remote device by factoring in a variety of parameters including operating system details, whether any security package is used within the remote device, and if other security best practices have been implemented or not. Versa's native ZTNA capabilities can be configured in full (forward or reverse) proxy mode to terminate remote device-initiated sessions and flows and scan them using a rich set of NGFW, UTM, SWG, ATP functionality.

The Versa instance can also be configured to provide detailed access control using built-in inline CASB functions and to scan for data for DLP purposes. Lastly, traffic to and from workloads can be micro-segmented based on dynamically assessed security posture, application, user, or other parameters.

Furthermore, since the Versa appliance is now installed in the compute appliance, the solution no longer requires extra space, power, nor additional cabling requirements. Thus, this reduces the physical footprint needed to support the compute, network, and security devices.

Theft risk mitigation

With respect to the risk of device theft, in addition to ensuring that the user implementing the remote device is a validated and trusted entity at the time of deployment, Versa Secure SD-WAN's feature set allows for the use of geolocation to define a security policy to limit the access of the remote device based upon the remote device's position. This could be very useful to deter acts of theft as once the geo-perimeter is violated, the device would become inoperable. Even in devices that are mobile, geolocation could be utilized to create regions of operation, and violation of those regions would enact security policies to prevent or limit access.

The SD-NIC can also be configured to use the TPM chip of the compute platform (if it has one) to create a secure authentication relationship between the compute platform and the SD-NIC. This addresses possible movement of the SD-NIC from one remote device to another, reducing the risk of bad actors attempting to spoof the genuine server. If the remote device does not have a TPM chip, a security profile can be created to prevent the Versa node from operating within a different remote device. Device fingerprinting would be used to create a host remote device profile, and the Versa instance would only allow that fingerprint profile to pass through the security posture.

Simplified management tools and policies

Traditionally, security appliances require one set of management tools, and routers and switches require another set of management tools, perhaps even a different management tool set per vendor. Increasing the set of management tools implies that the security policies need to be configured separately in each of the management tools, and when changes are made to the security policies, they need to be replicated to all the different management tools. Since the SD-NIC runs Versa's operating system natively, the Versa SD-NIC does not require any additional management tools if the customer has already deployed the Versa solution in any part their network.

Security policies can be instantiated for SD-WAN, SASE, ZTNA, or any other Versa offering from a centralized management tool. This simplifies policy creation, deployment and the compliance process. Versa's policy engine is capable of defining policies at a granular level. Policies can be written based on application, user, location, device, micro-segment, network, context (location, mobility, time), and many more criteria. This provides great flexibility when developing and implementing security postures.

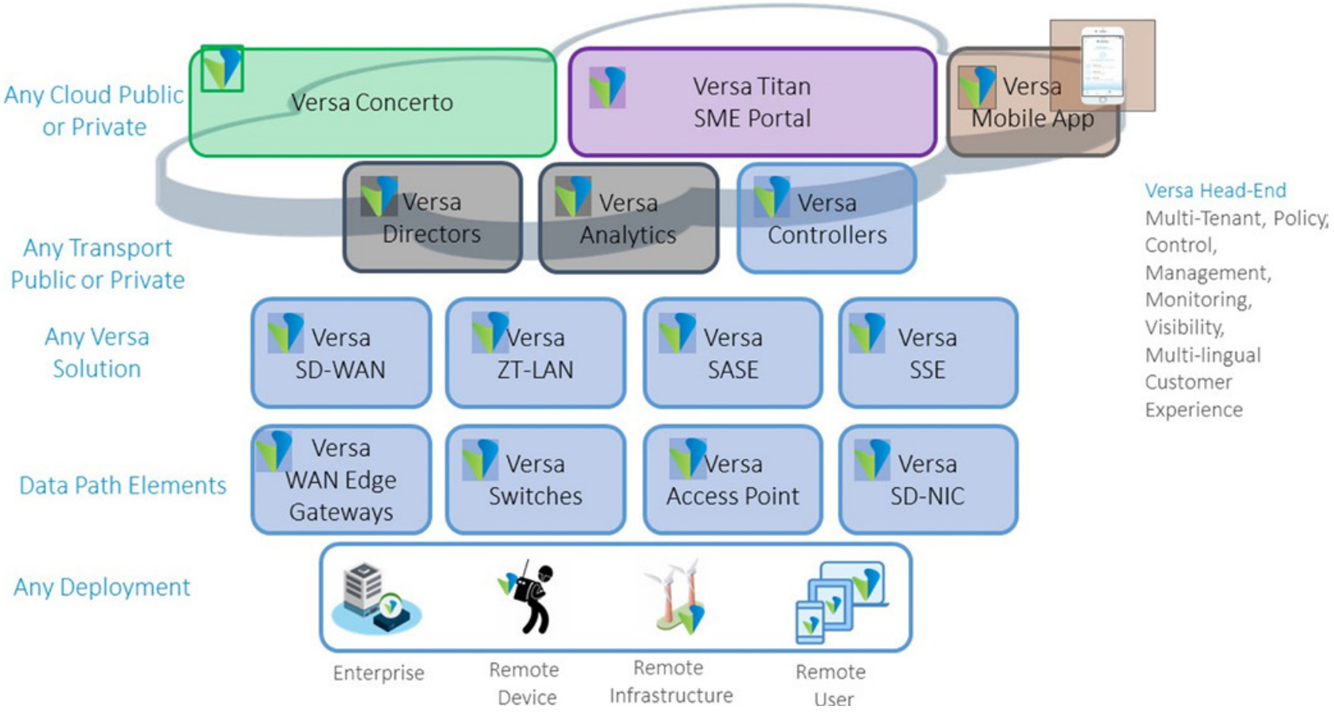


Figure 6- Centralized management allows for security policies to be applied uniformly, including to the SD-NIC and remote device.

Centralized management

As seen in Figure 6, the Versa management is centralized and controlled by Versa Director, Concerto and Controllers. Additionally, the information data store is centralized in the Versa Analytics. This centralized management design allows for security policies to be applied uniformly across VOS instances across the network and on the cloud to deliver SD-WAN, SD-LAN, ZTNA, SASE and SSE. Utilizing the Versa SD-NIC, these security policies extend into the remote and IOT devices. This Versa management complex can be hosted in any cloud computing environment or in the enterprise environment. Versa offers multiple methods for managing the Versa management environment: Versa hosted and managed, Versa hosted but customer-managed, customer-hosted and Versa-managed, or both customer-hosted and managed. In each of these scenarios, the management of the components can be a hybrid model where Versa performs some of the management and the customer performs the remaining tasks.

For more details on the Versa Secure SD-NIC or to request a demonstration, please visit https://www.versa-networks.com/products/sd-nic or contact a Versa sales representative.